UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/534,336	05/10/2005	Jurgen Bieber	2002P17424WOUS	2925

7590   09/01/2009

Siemens Corporation
Intellectual Property Department
170 Wood Avenue South
Iselin, NJ 08830

EXAMINER
AFOLABI, MARK O

ART UNIT	PAPER NUMBER
2454	

MAIL DATE	DELIVERY MODE
09/01/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
	10/534,336	BIEBER, JURGEN
Office Action Summary	Examiner	Art Unit
	MARK O. AFOLABI	2454

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 June 2009*.
2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *27-40* is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) *27-40* is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☐ All   b)☐ Some *   c)☐ None of:
      1.☐ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.
5)☐ Notice of Informal Patent Application
6)☐ Other: _____.

DETAILED ACTION

1.   This communication is considered fully responsive to the arguments and amendments filed on 06/17/2009 for the patent Application No. 10/534,336 filed 09/26/2003. Claims 27, 33, 36 and 37 are amended, and all claims 27-40 have been examined and remain pending.

Response to Arguments

2.   Applicants' arguments and amendments with respect to claims 27-40 have been fully considered and are persuasive in light of the amendments thereto. Accordingly, the rejections are withdrawn, and a new ground of rejection is presented below upon further consideration.

Claim Rejections - 35 USC S 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action: (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. The factual inquiries set forth in Graham v. John Deere Co., 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.

3. Resolving the level of ordinary skill in the pertinent art.

4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

5.   Claims 27, 28, 33, 35 and 36, are rejected under 35 U.S.C. 103(a) as being unpatentable over **Truong** et al. (US 6,151,609) **(Truong** hereafter) and **Schwerdtfeger** et al. (US 7,054,952) **(Schwerdtfeger** hereafter) in view of **Callaghan** et al. (US 5,737,523) **(Callaghan** hereafter).

Regarding claim 27, a server (server, Fig. 1—item 14) for developing, producing, or configuring an automation system, comprising:

    Truong teaches a storage system in the server (e.g. Fig. 2---item 44, 'storage', and the "Remote Internet server 15 includes a server memory 46, ...and a mass storage device 44, col. 7, ln 34-40), in which are stored in a first format files needed or created for the production or configuration of the automation system; and

    a communication interface (e.g., common gateway interface ("CGI")), in the server via which a remote client accesses the files (e.g., Remote editor program **40** may be implemented using a common gateway interface ("CGI") program, called a script, that receives the input from web browser **32** of client **12**, processes the input and executes other programs of remote Internet server **15** as necessary, and provides any results to web browser 32 in HTML format, col. 8, ln 10-17), wherein the interface comprises first means (e.g. Fig. 2---item 40, 'Remote Editor Program') for transmitting to one or more remote clients a

copy of selected ones of the files in a second format that can be processed by the remote client (i.e., I/O devices, col.6, ln 13-24) (e.g., receiving a file selection from the web browser at the server, the file selection identifying one of the files; and is communicating a copy of one of the files from the server to the web browser for editing, claim 7), and the interface comprises second means (e.g. Fig. 2---item 40, 'Remote Editor Program') for receiving files created or modified from each remote client (col. 8, ln 10-37, particularly, 23-29 and col. 1, ln 51 through col. 2 ln 20) and storing the received files into the storage system in the first format. (e.g., remotely editing files stored on a remote Internet server, abstract);

      Truong does not explicitly teach converting the received files into the first format.

      However**, Schwerdtfeger teaches** a method wherein the interface is embodied converting the received files into the first format (e.g., receives an electronic document in a first digital format (e.g., HTML or XML, abstract).

      Neither **Troung** nor **Schwerdtfeger** do not explicitly teach the underlined limitation of claim 27, 'Wherein the selected ones of the files in the second format are modified by the remote client.

      But, **Callaghan teaches** the underlined limitation, **w**herein the selected ones of the files in the second format are modified by the remote client (e.g., storing a given file system modifiable by clients of the server computer having an access status of read-write for the given file system readable by clients, col. 3, lines 34-46).

      Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention to add the features of **Schwerdtfeger** for producing or configuring an automation system wherein the system includes interface, which is embodied to convert the received files thereby allowing many different kinds of information to be seen by users of different devices, col. 1, lines, 5-40, Schwerdtfeger. Furthermore, **Callaghan**

features can be incorporated into **Troung** and **Schwerdtfeger** wherein the remote client is the one modifying the file by helping in conserving RAM for other software running on the server, col. 7, lines 19-43, Callaghan.

Regarding claim 28, wherein a plurality of clients access the files (e.g., Network interconnection **10** includes the interface between Internet server **14** and a plurality of clients, col. 5, ln 7-14 and col. 1, ln 31-40, Truong), and further comprising a security device in the server that authorizes (e.g., Fig. 5, 'Password' on Remote Editor System, Truong) a specific selection of the files to each of the clients by password interrogation (e.g., Fig. 3B—item 118, Truong).

Regarding claim 33, a server for engineering and configuring an automation system, comprising:

a memory in the server for storing files for engineering (e.g., col. 7, ln 34-40) and configuring the automation system, wherein the files are stored in a first format (e.g., first digital format (e.g., HTML or XML, abstract), Schwerdtfeger) that can be processed by the server (e.g., a remote editor system **(26)** is provided for remotely editing files stored on a remote Internet server **(15)**, Truong); and

an interface in the server for providing network access to the files by a client remote from the server (e.g., Remote editor program **40** may be implemented using a common gateway interface ("CGI") program, called a script, that receives the input from web browser **32** of client **12,** processes the input and executes other programs of remote Internet server **15** as necessary, and provides any results

to web browser 32 in HTML format, col. 8, ln 10-17, Schwerdtfeger),
wherein the interface comprises:

a first means (e.g. Fig. 2---item 40, 'Remote Editor Program',
Truong) for making a copy of selected files in the memory, converting the copy to a
second format (i.e., text string entered), that can be processed by the client and
transmitting the copy in the second format (i.e., translate the first
portion of document **12** from a first digital format (e.g., HTML)
to a script expressed in a second digital format (e.g., a
scripting language understood by a user agent **40** within client
machine **22**,, col. 7, ln 5-20, Schwerdtfeger) and

a second means (e.g. Fig. 2---item 40, 'Remote Editor
Program', Truong) for receiving files created or modified by the remote client,
(e.g., col. 1, lines, 13-30, Callaghan) converting the received files from
a received format into the first format (e.g., receiving a file selection
from the web browser at the server, the file selection
identifying one of the files; and is communicating a copy of one
of the files from the server to the web browser for editing,
claim 7, Truong), and storing them in the memory;

Wherein the selected ones of the files in the second format are modified by the
remote client (e.g., storing a given file system modifiable by
clients of the server computer having an access status of read-
write for the given file system readable by clients, col. 3,
lines 34-46).

Regarding claim 35, further comprising an access management device, which, if more
than one remote client accesses a file stored in the memory, only allows access
(e.g., a client machine coupled to (i.e., in wired or wireless

communication with) a transcoder proxy, col. 3, lines 13-52, particularly 13-22, Schwerdtfeger) by one of these remote clients (e.g., PDA, Schwerdtfeger).

Regarding claim 36, wherein a plurality of clients access the files (e.g., Network interconnection **10** includes the interface between Internet server **14** and a plurality of clients, col. 5, ln 7-14 and col. 1, ln 31-40), and further comprising a security device in the server that authorizes (e.g., Fig. 5, 'Password') each client access to a specific selection of files in the memory by password interrogation (e.g., col. 10, lines 9-20, Callaghan) of each client (e.g., Fig. 3A—item 118 and col. 8, lines 3-37, Truong) and an access management device in the server that keeps a log of which of the clients is accessing, which of the files, and provides conflict resolution when more than one client simultaneously requests access to a specific file (e.g., if client had read only access status and the file operation **26** required modifying the given file system **30**, the NFS server **200** could respond with an error message informing the **NFS** client **12** that the required write access status was lacking...By way of example, the **NFS** server **200** may record in a file and/or on a system terminal that an unauthenticated **NFS** request **22** was received from **NFS** client 12, col. 9, lines 9-56, esp. lines 15-31, Callaghan).

6. Claims 29-32 and 37-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Truong** (US 6,151,609) and **Schwerdtfeger** (US 7,054,952) and in view of **Callaghan** (US 5,737,523) in further view of **Vishlitzky** et al. (U 2003/0195886) (**Vishlitzky** hereafter).

Regarding claim 29:

Truong, Schwerdtfeger and Callaghan teach all the limitation of claims 27 for a server development or configuring remote client is embodied as a browser-based client and an access management device (e.g., col. 3, lines 53-67, Schwerdtfeger) in the server.

However, ***Truong, Schwerdtfeger and Callaghan fail to teach*** that resolves conflicts when first and second clients attempt to simultaneously access a given file by locking the given file for access by only the first client, and indicating a locked status to the second client.

Vishlitzky teach the resolves conflicts when first and second clients attempt to simultaneously access a given file by locking the given file for access by only the first client, and indicating a locked status to the second client (e.g., access to data may be controlled by a flag or lock that prohibits multiple processes having access to the data simultaneously, [0048], Vishlitzky) and indicating a locked status to the second client (e.g., [0048], Vishlitzky).

It would have been obvious to one of ordinary skill in the art at the time invention was made to apply the teachings of Truong, Schwerdtfeger and Callaghan for configuring an automation system with simultaneously accessing a given file by locking the given file for access. One would be motivated to embark on this procedure for security and make sure an updated file is maintained at all time to all users.

Regarding claim 30, wherein the access management device (e.g., col. 3, lines 53-67, Schwerdtfeger) prioritizes access to the given file by locking the given file for access by an earliest requesting client until the earliest requesting client

releases the file (e.g., a process accessing data may need to wait until
another process releases the data, [0048], Vishlitzky).

Regarding claim 31, wherein the access management device coordinates access to
the given file by locking the given file for access by an earliest requesting client until a
later requesting client requests the file, then notifies the earliest requesting client of the
later requesting client, and allows the earliest requesting client to choose to retain
access or release it (e.g., a hardware lock controls access to a software
lock (flag) so that a process first obtains control of the
hardware lock, tests the software lock, and then, if the
software lock is clear, the process sets the software lock and
then releases the hardware lock. If the process gets the
hardware lock and determines that the software lock is not
clear, then the process releases the hardware lock so that
another process that has set the software lock can clear the
software lock at a later time, [0048], Vishlitzky).
.

Regarding claim 32, wherein the access management device prioritizes access to the
given file by assigning different access priorities to different clients (e.g.,
providing dynamic distributed file system client authentication
within a distributed file system computing environment includes
the steps of receiving an **NFS** request from an NFS client,
determining whether the NFS client has an access status
sufficient to perform the NFS request. And performing the NFS
request when the NFS client has sufficient access status,
abstract, Callaghan), locks the given file for access by an earliest requesting
client until a later requesting client requests the given file, then compares the access

priorities of the earliest and later requesting clients, and if the later requesting client has higher access priority than the earliest requesting client, notifies the earliest requesting client that access to the given file will be switched to the later requesting client, otherwise continuing to reserve the given file for the earliest requesting client (e.g., [0048], `Vishlitzky`).

Regarding claim 37, wherein the access management device that resolves conflicts when first and second clients attempt to simultaneously access a given file by locking the given file for access by only the first client (e.g., `access to data may be controlled by a flag or lock that prohibits multiple processes having access to the data simultaneously, [0048],` Vishiltzky) and indicating a locked status to the second client (e.g., [0048], `Vishlitzky`).

Regarding claim 38, wherein the access management device prioritizes access to the given file by locking the given file for access by an earliest requesting client until the earliest requesting client releases the file (e.g., `a process accessing data may need to wait until another process releases the data, [0048], Vishlitzky).`

Regarding claim 39, wherein the access management device coordinates access to the given file by locking the given file for access by an earliest requesting client until a later requesting client requests the file, then notifies the earliest requesting client of the later requesting client, and allows the earliest requesting client to choose to retain access or release it (e.g., `a hardware lock controls access to a software lock (flag) so that a process first obtains control of the hardware lock, tests the software lock, and then, if the`

software lock is clear, the process sets the software lock and
then releases the hardware lock. If the process gets the
hardware lock and determines that the software lock is not
clear, then the process releases the hardware lock so that
another process that has set the software lock can clear the
software lock at a later time, [0048], Vishlitzky).

Regarding claim 40, wherein the access management device prioritizes access to the
given file by assigning different access priorities to different clients, locks the given file
for access by an earliest requesting client until a later requesting client requests the
given file, then compares the access priorities of the earliest and later requesting
clients, (e.g., Processing begins at a first step 172 where it is
determined if the particular track corresponding to the device
table entry being written is on the standard logical device or
the log device. If it is determined the particular track of
interest is on the standard logical device, control passes from
the step 172 to a step 178 where the track corresponding to the
device table entry being written is locked. Locking the track at
the step 178 prevents other processes from getting access to the
track, and from modifying the corresponding table entry, [0049],
Vishlitzky) and if the later requesting client has higher access priority than the
earliest requesting client, notifies the earliest requesting client that access to the given
file will be switched to the later requesting client, otherwise continuing to reserve the
given file for the earliest requesting client (e.g., If it is determined at the
test step 322 that one or more protection bits are set for the
tracks of the standard logical device that are being written,
control passes from the step 322 to a step 326, where the HA
sends a request to the DA indicating that protection bits are
set for the tracks. When the DA receives the request that is

sent at the step 326, the DA performs the operations set forth in the flow chart 300 of FIG. 11, [0070] and Fig. 11, Vishlitzky).

7.   Claim 34 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Truong** (US 6,151,609) and **Schwerdtfeger** (US 7,054,952) and in view of **Callaghan** (US 5,737,523) and in further view of **Lee** et al. (WO 2002-095954) **(Lee** hereafter).

Regarding claim 34:

Truong, Schwerdtfeger and Callaghan teach all the limitation of claim 33 and also the remote client is embodied as a browser-based client that communicates with the interface via an Internet or Intranet data line (e.g., ability to remotely access, view, edit, and save a server file using any client having a web browser and connected to the Internet., col. 3, ln 44-54, Truong);

the first and second means provide conversion means for graphics files and conversion means for text files (e.g., transcoder proxy **28** may convert graphics images within electronic document **12** from one format to another, col. 7, ln 11-26, Schwerdtfeger);

the conversion means (item 28 of Fig. 4) for graphics files converts graphics files stored in the memory into an SVG format (e.g., GIF formats to scaled vector graphicslSVG format, etc., Schwerdtfeger) that can be processed by the remote client (e.g., client 22 of Fig. 2, Schwerdtfeger) and vice versa (i.e., from one format to another) (col. 7, lines 11-25, Schwerdtfeger); and

However, ***Truong, Schwerdtfeger and Callaghan*** does not explicitly teach the underlined limitation for file format conversion mean for text files convert into a DHTML format, which can be processed by the remote client

But, **Lee teaches** the file format the conversion means (Fig. 1—item (1-4)
for text files converts the text files stored in the memory into a DHTML format that can
be processed by the remote client (abstract).

It would have been obvious to one of ordinary skill in the art at the time invention
was made to apply the teachings of Lee's conversion mechanism wherein the text files
are been converted into DHTML format for the remote clients to properly display
depending upon the type of device.

Conclusion

Any inquiry concerning this communication or earlier communications from the
examiner should be directed to MARK O. AFOLABI whose telephone number is (571)
270-5627. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's
supervisor, NATHAN FLYNN can be reached on 571-272-1915. The fax phone number
for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M.O.A/
/Mark O. Afolabi/
Examiner GAU 2454

/Nathan J. Flynn/
Supervisory Patent Examiner, Art Unit 2454